2412-135924RU

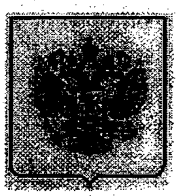
METHOD FOR ENCRYPTING AND TRANSMITTING SPEECH INFORMATION IN GSM-900, DCS-1800 CELLULAR MOBILE COMMUNICATIONS

Abstract

The invention relates to the field of encrypted communications equipment. The method allows confidentiality of transmitted speech information of subscribers in GSM-900 (DCS-1800) cellular mobile communications networks and impossibility to discredit this information in speech message interception in anyone of communications system interfaced. Said effect of interfaces is achieved by digitizing speech information, encoding the digitized speech information using a speech conversion algorithm; and further encrypting said encoded information by pair keys not known to third persons; and then transmitting said encrypted information from one subscriber to another through a duplex data (computer file) transmission channel assigned by the GSM-900 (DCS-1800) system. Simultaneously with reception, there are the steps of decrypting and detecting (that is, digital-to-analog converting) of said information) information coming from channel. With this, the speech converting and encrypting/decrypting function are realized in a special subscriber device interfacing standard radio equipment (mobile terminals) of subscribers via the serial RS-232 butting designed to couple a computer. In this case, a duplex "transparent" data transmission channel assigned by GSM-900 (DCS-1800) cellular mobile communications systems is used as a transport medium to transmit speech encryption. 2 Figs.

(19) RU (11) 2132597 (13) C1

(51) 6 H04Q7/32, H04L9/12



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

Статус: по данным на 29.04.2008 - действует

(21) Заявка: **98105818/09**

(22) Дата подачи заявки: **1998.03.25**

(45) Опубликовано: **1999.06.27**

(56) Список документов, цитированных в отчете о поиске: **WO 93/26103 A1, 23.12.93. US 5530959 A, 25.06.96. US 5349643 A, 20.09.94. GB 2261349 A, 12.05.93. FR 2719962 A1, 26.04.95. US 5649299 A, 15.07.97. US 5715552 A, 03.02.98. US 5623533 A, 22.04.97. EP 0750438 A1, 19.06.96. RU 95106218 A1, 20.01.97.**

(71) Заявитель(и): **Войсковая часть 43753**

(73) Патентообладатель(и): **Войсковая часть 43753**

Адрес для переписки: **121351, Москва, ул.Ельнинская, 1, в/ч 43753 Командиру части А.Алферову**

(54) СПОСОБ ШИФРОВАНИЯ И ПЕРЕДАЧИ ШИФРОВАННОЙ РЕЧЕВОЙ ИНФОРМАЦИИ В СЕТЯХ СОТОВОЙ ПОДВИЖНОЙ СВЯЗИ СТАНДАРТОВ GSM-900, DCS- 1800

Изобретение относится к области техники шифрованной связи. Способ позволяет обеспечить конфиденциальность передаваемой речевой информации абонентов в сетях сотовой подвижной связи стандартов GSM-900 (DCS-1800) и невозможность компрометации этой информации при перехвате зашифрованных сообщений в любом из интерфейсов системы связи. Указанный эффект интерфейсов достигается тем, что речевая информация преобразуется в цифровую форму, кодируется с использованием алгоритма речепреобразования и дополнительно зашифровывается на парных ключах, не известных третьим лицам, а затем в зашифрованном виде передается от абонента до абонента через предоставляемый системой GSM (DCS-1800) дуплексный канал передачи данных (компьютерных файлов). Одновременно на приеме осуществляется расшифрование и детектирование (из цифровой формы в аналоговую) приходящей из канала информации. Функции речепреобразования и шифрования/расшифрования при этом реализуются в специальном мобильном абонентском устройстве, которое сопрягается с штатным радиооборудованием абонентов (мобильными терминами) через асинхронный последовательный стык RS-232, предназначенный для подключения компьютера. В этом случае дуплексный "прозрачный" канал передачи данных, предоставляемый системами сотовой связи стандартов GSM-900 (DCS-1800), используется в качестве транспортной среды для передачи шифрования речи. 2 ил.

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

Изобретение относится к области техники шифрованной связи.

Уже известны способы шифрования дискретной речевой информации в сетях транкинговой и подвижной связи, реализованные в стандартах Tetra, GSM-900, DCS-1800 для защиты информации от компрометации путем перехвата в радиоканале. Эти способы основаны на преобразовании речевого сигнала в дискретную (цифровую) форму, кодировании с применением специального алгоритма речепреобразования, уменьшающего скорость информационного цифрового потока, содержащего речевые параметры, до 13 кбит/с (для стандартов GSM-900 и DCS-1800), с последующим его шифрованием (криптографическим преобразованием) в передающих трактах абонентского оборудования и в оборудовании базовых станций. Аналогичные преобразования, но в обратной последовательности, с заменой процедуры шифрования на расшифрование, производятся

в приемных трактах абонентского оборудования и оборудовании базовых станций при восстановлении исходного речевого сигнала и 13-ти килобитного цифрового информационного потока, содержащего параметры речи, соответственно (см. фиг. 1). Шифрование информации абонентов в указанных системах происходит только на участке радиоканала, т.е. между абонентом и обслуживающей его базовой станцией.

Поскольку заявленный способ предназначен для использования в сетях сотовой связи стандартов GSM-900 и DCS-1800, в качестве прототипа выбираем способ шифрования и передачи шифрованной речевой информации, реализованный в этих стандартах.

В стандартах GSM-900 и DCS-1800 для соединения сетевого оборудования используются различные интерфейсы, отличающиеся назначением, электрическими характеристиками, а также уровнем защиты передаваемой информации от компрометации. На фиг. 1 показано функциональное построение и основные интерфейсы системы сотовой связи стандарта GSM-900. Криптографическая защита (шифрование) речевой информации и данных (компьютерных файлов, факсов) осуществляется только на участке радиоинтерфейса (U_m-интерфейс), в остальных - внутрисетевых интерфейсах и в оборудовании сети информация циркулирует в открытом (незашифрованном) виде, что создает угрозу ее компрометации со стороны злоумышленников.

Ключи, на которых производится шифрование/расшифрование информации в абонентском и оборудовании (в базовой станции), генерируются в каждом сеансе связи на основе индивидуальных ключей пользователей, хранящихся в SIM-картах абонентских станций и базе данных сети. При вхождении в связь сеть проводит аутентификацию абонента (проверку права доступа в сеть и его полномочий) и одновременно вырабатывает в абонентском и сетевом оборудовании одинаковые сеансовые ключи шифрования/расшифрования. При этом в базе данных сети производится запрос индивидуальных атрибутов абонента, включая вычисляемый сеансовый ключ шифрования/расшифрования, и их пересылка по криптографически незащищенному интерфейсу из базы данных до конкретной базовой станции. В случае успешного завершения аутентификации, в процессе которой мобильная станция и сеть обмениваются специальными кодовыми посылками RAND и SRES, между мобильной и базовой станциями устанавливается канал связи, по которому передается информация, зашифрованная на идентичных сеансовых ключах K_c (фиг. 2).

Указанный механизм формирования ключей K_c обладает недостатком, заключающемся в возможности организации с помощью технических средств перехвата доступа к ключевой информации K_c и индивидуальным атрибутам абонента, передаваемым по криптографически незащищенным интерфейсам системы, что создает предпосылки для компрометации информации пользователя, передаваемой в зашифрованном виде по радиоканалу.

Описание мер безопасности, применяемых в сетях сотовой связи стандарта GSM-900 для защиты информации пользователей, приведено в /1/, /2/.

В сотовых сетях GSM-900 (DCS-1800) пользователям предоставляют, помимо услуг телефонной связи, возможность дуплексной асинхронной передачи/приема дискретных данных (компьютерных файлов) со скоростью до 9600 бит/с. Предоставляемый системой канал передачи данных может быть "прозрачным" для пользователя при выполнении необходимых настроек системы, таких как запрет использования протокола защиты от ошибок, запрещение повторной передачи кадров и др., что позволяет его использовать для организации шифрованной телефонной связи. В этом случае зашифрованный канал, по которому передается информация, устанавливается от одного участника связи до другого, без расшифрований информации в тракте сети связи. При этом процесс шифрования/расшифрования производится на парных ключах, не передаваемых по сети и, следовательно, недоступных третьим лицам.

Предложенное решение позволяет устранить присущие системам GSM-900 и DCS-1800 вышеуказанные недостатки.

Целью предлагаемого способа является обеспечение конфиденциальности передаваемой речевой информации абонентов в сетях сотовой подвижной связи стандартов GSM-900 (DCS-1800) и невозможность компрометации этой информации при перехвате зашифрованных сообщений в любом из интерфейсов системы связи.

Указанная цель достигается тем, что речевая информация преобразуется в цифровую форму, кодируются с использованием алгоритма речепреобразования и дополнительно зашифровывается на

парных ключах, не известных третьим лицам, а затем в зашифрованном виде передается от абонента до абонента через предоставляемый системой GSM (DCS) дуплексный канал передачи данных. Одновременно на приеме осуществляется расшифрование и декодирование (из цифровой формы в аналоговую) приходящей из канала информации. Функции речепреобразования и шифрования/расшифрования при этом реализуются в специальном мобильном абонентском устройстве, которое сопрягается со штатным радиооборудованием абонентов (мобильными терминалами) через асинхронный последовательный стык RS-232, предназначенный для подключения компьютера. В этом случае дуплексный, "прозрачный" канал передачи данных (компьютерных файлов), предоставляемый в системах связи стандартов GSM-900 (DCS-1800), используется в качестве транспортной среды для передачи шифрованной речи.

Использование штатного речевого канала системы связи стандарта GSM для передачи сообщений через весь тракт от абонента до абонента не представляется возможным, т.к. в этом канале не обеспечивается взаимная однозначность преобразования случайной последовательности символов (какой является шифртекст) на входе и выходе узла преобразования, так называемого транскодера, предназначенного для выравнивания скоростей и преобразования поступающих от оборудования базовых станций цифровых потоков речевой информации в многоканальный ИКМ сигнал и обратно.

Литература

1. Громаков Ю.А. Стандарты и системы подвижной радиосвязи, - М.: Мобильные телесистемы и Эко-Трендз, 1997, 240 с.

2. An introduction to GSM/ Siegmund M. Redl, Matthias K. Weber, Malcolm W. Oliphant, ISBN 0-89006-785-6, 1995, 380 p.

ФОРМУЛА ИЗОБРЕТЕНИЯ

Способ шифрования и передачи шифрованной речевой информации в сетях сотовой подвижной связи стандартов GSM-900, DCS-1800, заключающийся в преобразовании речевых сигналов в цифровую форму и кодировании цифрового потока с использованием алгоритма сжатия речи с последующим его шифрованием на передаче и соответствующим расшифрованием и декодированием на приеме в абонентских радиотелефонных устройствах сотовой подвижной связи стандартов GSM-900, DCS-1800, отличающийся тем, что речевые сигналы, преобразованные в цифровую форму, в мобильном абонентском устройстве дополнительно шифруются на ключах парной связи, не известных третьим лицам, и в зашифрованном виде передаются через связной тракт системы по "прозрачному" дуплексному каналу передачи данных от абонента до абонента с последующим расшифрованием на идентичных ключах и восстановлением исходного речевого сигнала в приемном абонентском устройстве.

ИЗВЕЩЕНИЯ К ПАТЕНТУ НА ИЗОБРЕТЕНИЕ

Код изменения правового статуса	**NF4A - Восстановление действия патента РФ на изобретение (датой восстановления действия патента является дата публикации данного бюллетеня)**
Дата публикации бюллетеня	**2004.05.10**
Номер бюллетеня	**13/2004**

Код изменения правового статуса	**MM4A - Досрочное прекращение действия патентов РФ из-за неуплаты в установленный срок пошлин за поддержание патента в силе**
Дата публикации бюллетеня	**2004.05.27**
Номер бюллетеня	**15/2004**
Дата прекращения действия патента	**2003.03.26**

РИСУНКИ